CLAIMS

1. A method of managing security keys provided to users of a service comprising the steps of:

issuing a security key to a first user eligible to receive the service;

monitoring the first user's status to establish whether the first user is eligible to receive the service;

establishing, in accordance with a policy, a first value associated with invalidation of the first user's key, and a second value associated with providing the service to an ineligible user, and if the second value exceeds the first value, invalidating the key.

2. A method according to claim 1 wherein the policy further provides that the first value is related to the economic penalty associated with reconfiguration of keys issued to other users consequent to invalidation of the first user's key.

3. A method according to claim 1 wherein the policy provides that the second value is related to the economic penalty associated with provision of the service to the ineligible user.

4. A method according to claim 3 wherein the second value is calculated by aggregating the economic penalty associated with provision of the service to each ineligible user.

5. A method according to 4 wherein the economic penalty associated with provision of service to ineligible users includes a value representative of dilution of economic value to eligible users consequent to provision of the service to ineligible users.

6. A method according to claim 3 wherein the economic penalty of providing the service to ineligible users includes any costs arising from the provision of network and server capacity to ineligible users.

7. A method according to claim 2 wherein security keys are generated in an ancestrally-based hierarchy, and wherein invalidation of a given key necessitates a need for reconfiguration of each key in the hierarchy.

8. A method according to claim 7 wherein upon invalidation of a given key, an other key requires reconfiguration only to the extent that it shares common ancestor keys with the given invalidated key.

9. A method according to claim 8 wherein the hierarchy is a binary tree.

10. A method of managing provision of security keys to a plurality of users of a network service comprising the steps of:

generating plurality of security keys, each of which is related ancestrally to at least one other key of the plurality;

issuing keys to users;

monitoring users' status to for continuing eligibility for consumption of the service; and

upon establishing ineligibility of a user, determining upon the basis of a predetermined policy, a value for economic disbenefit to a provider of the service of: (a) invalidation of the ineligible user's key; and (b) provision of service to an ineligible user.

11. A method according to claim 10 further comprising the step of invalidating the key if the disbenefit of providing service to an ineligible user is greater than the disbenefit of invalidating the key.

12. A method according to claim 11 further comprising the step of aggregating the disbenefit of providing service to each ineligible user, and invalidating the key only if the aggregated disbenefit of providing the service to all ineligible users is greater than the disbenefit of invalidating the key.

13. A method according to claim 10 wherein invalidation of the key necessitates reconfiguration of each other key to the extent another key shares common ancestry with the invalidated key.